

The University of Chicago

ON SUMS OF VALUES OF A POLYNOMIAL
MULTIPLIED BY CONSTANTS

A PART OF A DISSERTATION SUBMITTED
TO THE FACULTY OF THE DIVISION OF
THE PHYSICAL SCIENCES IN CANDIDACY FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS
1935

By
KENNETH SMITH GHENT

Private Edition, Distributed by
THE UNIVERSITY OF CHICAGO LIBRARIES
CHICAGO, ILLINOIS

Reprinted from
DUKE MATHEMATICAL JOURNAL
Vol. 3, No. 3, 1937

The University of Chicago

ON SUMS OF VALUES OF A POLYNOMIAL
MULTIPLIED BY CONSTANTS

A PART OF A DISSERTATION SUBMITTED
TO THE FACULTY OF THE DIVISION OF THE
PHYSICAL SCIENCES IN CANDIDACY FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

1935

By
KENNETH SMITH GHENT

Private Edition, Distributed by
THE UNIVERSITY OF CHICAGO LIBRARIES
CHICAGO, ILLINOIS

Reprinted from
DUKE MATHEMATICAL JOURNAL
Vol. 3, No. 3, 1937





Digitized by the Internet Archive
in 2026

SUMS OF VALUES OF A POLYNOMIAL MULTIPLIED BY CONSTANTS

BY KENNETH S. GHENT

1. **Introduction.** We seek conditions on the integer s , on the sets of positive integers $(a_1, \dots, a_s)$ and on the coefficients of a polynomial $P(x)$ for which the Diophantine equation

$$(1) \quad n = \sum_{\nu=1}^s a_{\nu} P(h_{\nu})$$

is solvable in integers $h_{\nu} \geq 0$ for every integer n sufficiently large. By n sufficiently large we mean that n is greater than an existing constant b_1 which depends only on $s, a_1, \dots, a_s$ and on the degree k and the coefficients of the polynomial $P(x)$. We consider two cases of the polynomial $P(x)$:

$$(2) \quad P(x) = a(x^3 - x)/6 + b(x^2 - x)/2 + cx + d,$$

where $a > 0$ and a, b, c and d are integers;¹

$$(3) \quad \begin{aligned} P(x) = & ax(x+1)(x+2)(x+3)/24 + bx(x+1)(x+2)/6 \\ & + cx(x+1)/2 + dx + e, \end{aligned}$$

where $a > 0$ and a, b, c, d and e are integers.²

For $a_1 = \dots = a_s = 1$, the problem is the classical Waring problem for third and fourth degree polynomials. If $P(x)$ in (2) is such that $a \not\equiv 4c \pmod{8}$ James has shown that every sufficiently large integer n is a sum of nine values of $P(x)$.³ We show that for $s = 9$ and for integral constants $(a_1, \dots, a_s)$ satisfying certain congruential conditions given later, every sufficiently large integer can be expressed in the form (1). For $P(x)$ as in (3), Miss Humphreys has given conditions which are sufficient to prove that every sufficiently large integer n is expressible as the sum of 21 values of $P(x)$. Under certain further assumptions on $P(x)$ and on the sets of positive integers $(a_1, \dots, a_s)$ we shall

Received June 26, 1936; in revised form, June 28, 1937.

¹ A cubic polynomial in x is an integer for all integers $x \geq 0$ if and only if it is of the form (2)—R. D. James, *The representation of integers as sums of values of cubic polynomials*, American Journal of Mathematics, vol. 56 (1934), pp. 303–315. See also D. H. Hilbert, *Über die Theorie der algebraischen Formen*, Mathematische Annalen, vol. 36 (1890), pp. 511–512.

² A fourth degree polynomial in x is an integer for all integers $x \geq 0$ if and only if it is of the form (3). See M. G. Humphreys, *On the Waring problem with polynomial summands*, this Journal, vol. 1 (1935), pp. 361–375. The proof is accomplished by a slight modification of that of Hilbert in the paper previously cited.

³ James, loc. cit.

show that every sufficiently large integer n can be expressed in the form (1) for $s = 21$.

The proof depends on certain analytic theorems and on certain congruential theorems. The analytic theorems follow closely those of James⁴ and Landau.⁵ We quote the analytic theorems without proof;⁶ the congruential theory is given in detail.

2. Notations. The following notations are used throughout this paper. Further notations will be introduced when required.

$$K = 2^{k-1}; \quad \mathfrak{K} = 1 - 1/K; \quad f_v(x) = \sum_{h=0}^{\infty} x^{a_v P(h)};$$

$r(n) = r(n, k, s, a_1, \dots, a_s; a, b, c, d, e)$ = the number of solutions of (1); ρ denotes a primitive q -th root of unity;

$$S(a_v, \rho) = \sum_{h=r+1}^{r+m} \rho^{a_v P(h)};$$

$$S_{\nu_p} = \sum_h \rho^{a_v P(h)},$$

where h ranges over a complete set of residues mod q ;

$$A_0(q) = \frac{1}{q^s} \sum_{\rho(q)} \prod_{v=1}^s S_{\nu_p} \rho^{-n};$$

$\mathfrak{S}_0 = \mathfrak{S}_{0n} = \sum_{q=1}^{\infty} A_0(q)$ will be referred to as the Singular Series;

$$(a, b) = \text{g.c.d. of } a \text{ and } b.$$

3. Principal analytic theorem. Consider the following polynomial

$$(4) \quad \Phi(x) = \alpha_0 x^k + \alpha_1 x^{k-1} + \dots + \alpha_k,$$

where $\alpha_0 > 0$ and $\alpha_0, \alpha_1, \dots, \alpha_k$ are integers. The value α_s considered will be that of the first Hardy-Littlewood theory. The notations of the previous section are used with $P(x)$ replaced by $\Phi(x)$. Consider also equation (1) with $P(x)$ replaced by $\Phi(x)$. The theorem which follows can then be proved for the polynomial $\Phi(x)$ of degree k by a generalization of the proof given by Landau.⁷

THEOREM 1. For $s \geq (k - 2)K + 5$

$$\left| r(n) - \frac{\alpha_0^{-s/k} \Gamma^s(1 + 1/k)}{(a_1 \dots a_s)^{2/k} \Gamma(s/k)} \mathfrak{S}_0 n^{s/k-1} \right| < C_{20} n^{s/k-1-B_5},$$

⁴ James, op. cit.

⁵ E. Landau, *Über die neue Winogradoffsche Behandlung des Waringschen Problems*, Mathematische Zeitschrift, vol. 31 (1929), pp. 319-338.

⁶ Proofs of the analytic theorems are given in the writer's doctoral dissertation at the University of Chicago, August, 1935.

⁷ Landau, op. cit.

where C_{20} is a constant depending only on Φ , s and $\max a_v$ and B_5 is a constant depending only on k .

4. Primitive solutions. Consider $\Phi(x)$ as in (4). Let θ be the highest power of the prime p which divides every coefficient of $\Phi'(x)$. Then

$$\Phi_0(x) = p^{-\theta} \Phi'(x)$$

has at least one coefficient prime to p . We define γ as follows:

$$\gamma = \theta + 1 \text{ for } p > 2,$$

$$= \theta + 2 \text{ for } p = 2.$$

Let $M_0(m) = M_0(m, n)$ denote the total number of solutions of

$$(5) \quad \sum_{v=1}^s a_v \Phi(x_v) \equiv n \pmod{m}, \quad 0 \leq x_v < n.$$

For $m = p^l$, let $N_0(p^l, n)$ denote the number of solutions of (5) for which $p \nmid \text{g.c.d. of } \Phi_0(x_v)$. Let $N_{sp}(p^l, n)$ denote the number of solutions with $p \nmid \text{g.c.d. of } a_v \Phi_0(x_v)$. The last solutions defined will be referred to as primitive solutions. By generalizations of the work of Landau and James previously referred to, the following three lemmas can be proved.

LEMMA 1. If $l \geq \gamma$ then

$$N_{sp}(p^l) = p^{(l-\gamma)(s-1)} N_{sp}(p^\gamma).$$

LEMMA 2.

$$M_0(m) = m^{s-1} \sum_{q|m} A_0(q).$$

LEMMA 3. If p_h denotes the h -th prime, then

$$\sum_{q|p_1^l \cdots p_l^l} A_0(q) = \prod_{p \leq p_l} \sum_{q|p^l} A_0(q).$$

The following lemma is also required.

LEMMA 4. For $\epsilon \geq 0$

$$A_0(q) > -E_2 q^{-5/4+\epsilon},$$

where E_2 is a constant depending at most on $k, s, \alpha_0, \dots, \alpha_k, a_1, \dots, a_s$.

5. Application to the cubic and to the quartic. The analytic theorem and the lemmas that we have stated apply to a polynomial $\Phi(x)$ of degree k with integral coefficients and leading coefficient positive. The polynomials $P(x)$ of (2) and (3) have leading coefficient positive but the coefficients are not integers. Hence, for these cases, let $Q(x) = Q(x; v, t) = P(xv + t)$, where $t \geq 0$ and $v > 0$ are definite integers depending on the coefficients of $P(x)$ in the respective cases. We choose v so that it contains the least number of factors required to

make $Q(x)$ a polynomial with integral coefficients. The choice of t depends more specially on the case under consideration. For $Q(x)$ we define θ as before. For both the cubic and the quartic, $p > 3$ implies $\theta = 0$ since p does not divide all coefficients of $P(x)$.

6. Introduction to the congruential theory. The main portion of this paper is devoted to the development of certain congruential theorems⁸ for the polynomials (2) and (3). We are then able, with the aid of the analytic theory introduced, to prove the principal results given in Theorems 3 and 5. We assume that the cubic is not of the type excepted by James⁹ and that the quartic is not of the type excepted by Miss Humphreys.¹⁰

The following definition will be used: For a prime p and a positive integer l , a set of positive integers $(a_1, \dots, a_s)$ has the property $S(p, p^l)$ if one of the set $(a_1, \dots, a_s)$ which we may designate by a_i is prime to p and if the a_i ($i = 1, \dots, s$; $i \neq j$) are such that for every integer n there exists a $t < s$ for which

$$\sum_{i=1}^t a_i \equiv n \pmod{p^l}$$

is solvable.

7. Results for cubic polynomials. We seek conditions on the coefficients of $P(x)$ in (2) and on the constants $(a_1, \dots, a_9)$ under which the equation (1) is solvable in integers $h_\nu \geq 0$ for all sufficiently large integers n . We may evidently assume $d = 0$ in (2). We may also assume that a, b, c have no common factor other than unity; for if $p \mid a, p \mid b$ and $p \mid c$, then $p \mid P(x)$ and $\sum_{\nu=1}^s a_\nu P(x_\nu)$ would represent only multiples of p .

We first prove Theorem 2, a congruential theorem for the cubic; and then by Lemma 5 we obtain Theorem 3, the final theorem for the cubic. We state these theorems as follows for $P(x)$ as in (2).

THEOREM 2. *If the polynomial $P(x)$ and the set of positive integers $(a_1, \dots, a_s)$ satisfy the following three conditions:*

- (a) *for every prime $p > 3$, at least six of the positive integers $(a_1, \dots, a_s)$ are prime to p ;*
 - (b) *the set $(a_1, \dots, a_s)$ has the properties $S(2, 2^3)$ and $S(3, 3^2)$;*
 - (c) *$a \not\equiv 4c \pmod{8}$, i.e., the polynomial is not of the type excepted by James;*
- then for every integer n and for $Q(x) = P(vx + t)$ there exist primitive solutions of the congruence*

$$(6) \quad \sum_{i=1}^{s \geq 9} a_i Q(x_i) \equiv n \pmod{p^7}.$$

⁸ The methods of proof are similar to those of L. E. Dickson, *Cyclotomy, higher congruences and the Waring's problem*, American Jour. of Math., vol. 57 (1935), pp. 391-424.

⁹ Loc. cit.

¹⁰ Loc. cit.

THEOREM 3. *Let $s \geq 9$ be an integer; and let $P(x)$ and the set of positive integers $(a_1, \dots, a_s)$ be such that the conditions (a), (b), and (c) of Theorem 2 are satisfied. Then there exists a number C_{40} depending only on s, a, b, c and $a_1, \dots, a_s$ such that every integer $n > C_{40}$ is expressible in the form*

$$n = \sum_{\nu=1}^{s \geq 9} a_{\nu} P(x_{\nu}), \quad x_{\nu} \geq 0.$$

8. Congruential theory for cubic polynomials. We first consider (6) for primes $p > 3$. In §5 we saw that $\theta = 0$ for $p > 3$, hence $\gamma = 1$. Consider the polynomial $Q(x)$ in the form

$$(7) \quad Q(x) = A_1 x^3 + A_2 x^2 + A_3 x,$$

where A_1, A_2, A_3 are integers whose g.c.d. is unity. Suppose, first, that $A_1 \equiv 0 \pmod{p}$. Then the congruence is a second degree congruence which can be treated directly. Hence suppose $A_1 \not\equiv 0 \pmod{p}$. Then we may evidently take $A_1 \equiv 1 \pmod{p}$ since, if we determine d by $dA_1 \equiv 1 \pmod{p}$, dn ranges with n in (6) over all residues $\pmod{p}$. Let $a_1, \dots, a_6$ be six members of the set $(a_1, \dots, a_s)$ which are prime to the given prime p . Then each a_i ($i = 1, \dots, 6$) satisfies one of the congruences in

$$(8) \quad a_i \equiv x^3, \quad a_i \equiv gx^3, \quad a_i \equiv g^2x^3 \pmod{p},$$

where g is a fixed primitive root of p . Hence without loss of generality assume

$$(9) \quad a_1 \equiv a_2 u_1^3, \quad a_3 \equiv a_4 u_3^3 \pmod{p}.$$

Case 1. $A_2 A_3 (a_1 + a_2)(a_3 + a_4) \not\equiv 0 \pmod{p}$. Let $x_2 = -u_1 x_1$. Then

$$\begin{aligned} a_1 Q(x_1) + a_2 Q(x_2) &\equiv a_2(u_1^3 x_1^3 + x_2^3) + A_2(a_2 u_1^3 x_1^2 + a_2 x_2^2) + A_3(a_2 u_1^3 x_1 + a_3 x_2) \\ &\equiv a_2(u_1^3 x_1^3 - u_1^3 x_1^3) + A_2 a_2(u_1^3 x_1^2 + u_1^2 x_1^2) + A_3 a_2(u_1^3 x_1 - u_1 x_1) \\ &\equiv A_2 a_2(u_1^3 + u_1^2)x_1^2 + A_3 a_2(u_1^3 - u_1)x_1 \pmod{p}. \end{aligned}$$

Similarly, let $x_4 = -u_3 x_3$. Then

$$a_3 Q(x_3) + a_4 Q(x_4) \equiv A_2 a_4(u_3^2 + u_3^3)x_3^2 + A_3 a_4(u_3^3 - u_3)x_3 \pmod{p}.$$

Next¹¹ let $x_1 = X_1 + z$, where z is such that

$$(2A_2 a_2(u_1^3 + u_1^2))z + A_3 a_2(u_1^3 - u_1) \equiv 0 \pmod{p}.$$

This has one solution, since, from hypothesis, $2A_2 a_2(u_1^3 + u_1^2)$ is not divisible by p . Similarly, set $x_3 = X_3 + v$, where v is such that

$$2A_2 a_4(u_3^3 + u_3^2)v + A_3 a_4(u_3^3 - u_3) \equiv 0 \pmod{p}.$$

¹¹ If $A_3 a_2(u_1^3 - u_1) \equiv 0 \pmod{p}$, this transformation is unnecessary.

We have then essentially

$$(10) \quad \sum_{i=1}^4 a_i Q(x_i) \equiv rx^2 + sy^2 \equiv n \pmod{p},$$

where neither r nor s is divisible by p . This congruence is solvable for every integer n .

*Case 2.*¹² $A_2 A_3 \not\equiv 0 \pmod{p}$, $a_1 + a_2 \equiv 0 \pmod{p}$. Let $x_1 = x_2 + l$, where l is so chosen that $3l + A_2 \not\equiv 0 \pmod{p}$. Then

$$\begin{aligned} a_1 Q(x_1) + a_2 Q(x_2) &= a_1 Q(x_2 + l) + a_2 Q(x_2) \\ &= (a_1 + a_2)Q(x_2) + a_1(x_2^2(3l + A_2) + x_2(3l^2 + 2lA_2 + A_3) \\ &\quad + (l^3 + l^2A_2 + lA_3)); \end{aligned}$$

$$a_1 Q(x_1) + a_2 Q(x_2) \equiv a_1(3l + A_2)x_2^2 + a_1(3l^2 + 2lA_2 + A_3)x_2 + \text{const} \pmod{p}.$$

The remainder of the proof is as in Case 1.

Case 3. $A_2 A_3 \equiv 0 \pmod{p}$. We show that in this case we can make a transformation, $x = X + l$, which carries $Q(x)$ to

$$\begin{aligned} Q_1(x) &= X^3 + A_2'X^2 + A_3'X + \text{const} \\ &= X^3 + X^2(3l + A_2) + X(3l^2 + 2A_2l + A_3) + \text{const} \end{aligned}$$

in which $A_2' A_3' \not\equiv 0 \pmod{p}$. Suppose first that A_2 and A_3 are both divisible by p . Choose l prime to p and we have $A_2' A_3'$ not divisible by p as desired. Suppose next that A_2 is divisible by p but that A_3 is not divisible by p . Now

$$(11) \quad (3l^2 + A_3) \equiv 0 \pmod{p}$$

has at most two incongruent solutions for l . Hence there are at least $(p - 2)$ incongruent values of l for which (11) is not satisfied. Any one of these $(p - 2)$ values of l makes $A_2' A_3' \not\equiv 0 \pmod{p}$. Finally, suppose that A_2 is not divisible by p but that A_3 is divisible by p . There is a unique value of $l \pmod{p}$ for which $3l + A_2$ is divisible by p . One of the remaining $(p - 1)$ incongruent residues $\pmod{p}$ satisfies

$$3l + 2A_2 \equiv 0 \pmod{p}.$$

Hence there exist $(p - 2)$ incongruent values of l for which

$$(3l + A_2)(3l + 2A_2) \not\equiv 0 \pmod{p}.$$

We use one of these values of l in the transformation and we obtain $A_2' A_3' \not\equiv 0 \pmod{p}$.

Hence in all cases we can satisfy the condition that $A_2 A_3$ be not divisible by p .

We require a primitive solution of (6); i.e., at least one $a_i Q_0(x)$ prime to p . Suppose that no one of the $a_i Q(x_i)$ which we have used satisfies the desired condition. Then choose x_5 so that $a_5 Q_0(x_5)$ is prime to p . This we can do

¹² If $a_3 + a_4 \equiv 0 \pmod{p}$, the treatment is the same as when $a_1 + a_2 \equiv 0 \pmod{p}$.

since we have just seen that if A_3 is divisible by p we can make a transformation on x to give $Q_1(x)$ in which A_3' is not divisible by p ; and let x_5 be divisible by p . Then $a_5Q(x_5)$ is divisible by p while $a_5Q_0(x_5) \equiv a_5A_3 \pmod{p}$ is not divisible by p .

We have then shown that for $p > 3$ there exist primitive solutions of the congruence

$$\sum_{i=1}^6 a_i Q(x_i) \equiv n \pmod{p}$$

if for every prime $p > 3$, $a_1, \dots, a_6$ are all prime to p . We have thus proved Theorem 2 for primes $p > 3$.

For $p \leq 3$, James used in the congruence (6) fewer than 9 equal values of the polynomial and, if necessary, one additional value of the polynomial which insured that the primitivity condition be satisfied in order to solve the congruence for an arbitrary integer n . If we assume that our set $(a_1, \dots, a_s)$ has the properties $S(2, 2^3)$ and $S(3, 3^2)$, the discussion given by James applies to the present problem.¹³ We have thus proved Theorem 3.

9. Results for the quartic polynomial. We consider $P(x)$ as in (3). As in the case of the cubic polynomial, we may assume that a, b, c, d and e have no common factor other than unity. We prove Theorem 4, a congruential theorem for the quartic similar to Theorem 2 for the cubic, and give in Theorem 5 our final results for the quartic.

THEOREM 4. *If the polynomial $P(x)$ and the set of positive integers $(a_1, \dots, a_s)$ satisfy the following conditions:*

- (a) *for every prime $p > 3$, eleven of the constants $(a_1, \dots, a_s)$ are prime to p ;*
 - (b) *the set $(a_1, \dots, a_s)$ has the properties $S(2, 2^4)$ and $S(3, 3^2)$;*
 - (c) *the coefficient of x in the normal form¹⁴ of the polynomial is not divisible by a prime of the form $4m + 3$ ($p > 3$);*
 - (d) *the polynomial is not of the kind excepted by Miss Humphreys,*
- then for every integer n and for $Q(x) = P(vx + t)$ there exist primitive solutions of the congruence*

$$(12) \quad \sum_{i=1}^{s=21} a_i Q(x_i) \equiv n \pmod{p^\gamma}.$$

THEOREM 5. *Let $s \geq 21$ be an integer; and let $P(x)$, the quartic polynomial in (3), and the set of positive integers $(a_1, \dots, a_s)$ be such that the conditions (a), (b), (c), (d) of Theorem 4 are satisfied. Then there exists a constant C_{41} depending on s, a, b, c, d and $\max a_v$ such that every integer $n > C_{41}$ is expressible in the form*

$$n = \sum_{v=1}^s a_v P(x_v).$$

¹³ Our hypothesis makes Lemmas 12, 13, and 14 of James' paper available for our discussion. The use of Lemma 8 can be avoided. Sections 5 and 6 of James' paper then give the desired result.

¹⁴ The normal form of the polynomial is discussed in the next section.

10. **Congruential theory for the quartic.** Suppose that $Q(x)$ is of the form

$$Q(x) = \beta_0 x^4 + \beta_1 x^3 + \beta_2 x^2 + \beta_3 x + \beta_4,$$

where β_i ($i = 0, 1, \dots, 4$) are integers and $\beta_0 > 0$. This we can assume after transformation of $P(x)$ in (3) by replacing x by $vx + t$. As in the case of the cubic we may assume that $\beta_0 \equiv 1 \pmod{p}$. Moreover, if k is prime to p (this is the case for $p > 3$) we replace x by $X + z$ where z is so chosen that the coefficient of X^3 is divisible by p . Finally, after this transformation, we may evidently assume that the constant term is zero and consider (12) for $Q(x)$ replaced by

$$Q_1(x) = x^4 + A_2 x^2 + A_3 x.$$

We call $Q_1(x)$ the normalized form of the polynomial $Q(x)$. Then condition (c) of Theorem 4 implies $A_3 \not\equiv 0 \pmod{p = 4m + 3, p > 3}$.

We consider the congruence (12) for primes $p > 3$. Then $\theta = 0$ and $\gamma = 1$. Hence we consider

$$(13) \quad \sum_{i=1}^{s=21} a_i Q_1(x_i) \equiv n \pmod{p},$$

where we assume that $(a_1, \dots, a_{11})$ are prime to p . By Lemma 39 of a paper by Huston,¹⁵ there exist primitive solutions of

$$\sum_{i=1}^5 a_i h_i^4 \equiv n \pmod{p}.$$

Put $x_i = h_i y_1$ ($i = 1, \dots, 5$), $x_i = h_i y_2$ ($i = 6, \dots, 10$), where y_1 and y_2 are prime to p and where the h_i are so chosen that

$$(14) \quad \sum_{i=1}^5 a_i h_i^4 \equiv 0 \equiv \sum_{i=6}^{10} a_i h_i^4 \pmod{p},$$

and in each congruence at least one $a_i h_i$ is prime to p .

Case 1. $A_2 A_3 \not\equiv 0 \pmod{p}$. Suppose first that the values of h_i ($i = 1, \dots, 5$) which we have chosen to satisfy $\sum_{i=1}^5 a_i h_i^4 \equiv 0 \pmod{p}$ also satisfy $\sum_{i=1}^5 a_i h_i^2 \equiv 0 \pmod{p}$. Then by choice of h_1 or $-h_1$ we can have $\sum_{i=1}^5 a_i h_i$ not divisible by p . This is true since we may take $a_1 h_1$ prime to p and since if $(h_1, \dots, h_5)$ satisfies

$$\sum_{i=1}^5 a_i h_i^4 \equiv \sum_{i=1}^5 a_i h_i^2 \equiv \sum_{i=1}^5 a_i h_i \equiv 0 \pmod{p},$$

then $(-h_1, h_2, \dots, h_5)$ satisfies the first two congruences but insures that $\sum_{i=1}^5 a_i h_i$ is not divisible by p . Hence

¹⁵ R. E. Huston, *Asymptotic generalizations of Waring's theorem*, Proceedings of the London Mathematical Society, (2), vol. 39 (1935), pp. 82-115.

$$\sum_{i=1}^5 a_i Q_1(x_i) \equiv \sum_{i=1}^5 a_i h_i y_1 \equiv n \pmod{p},$$

which is solvable for every integer n . To satisfy the condition that the solution be primitive it may be necessary to add one more summand, $a_6 Q_1(x_6)$, where x_6 is divisible by p while

$$a_6 Q_1'(x_6) \equiv a_6(4x^3 + 2A_2x + A_3) \not\equiv 0 \pmod{p},$$

since p does not divide A_3 .

Suppose next that the values of h_i ($i = 1, \dots, 10$) which we have chosen to satisfy (14) are such that

$$\sum_{i=1}^5 a_i h_i^2 \not\equiv 0, \quad \sum_{i=6}^{10} a_i h_i^2 \not\equiv 0 \pmod{p}.$$

Then

$$\begin{aligned} \sum_{i=1}^{10} a_i Q_1(x_i) &\equiv A_2 \left(\sum_{i=1}^5 a_i h_i^2 \right) y_1^2 + A_3 \left(\sum_{i=1}^5 a_i h_i \right) y_1 \\ &\quad + A_2 \left(\sum_{i=6}^{10} a_i h_i^2 \right) y_2^2 + A_3 \left(\sum_{i=6}^{10} a_i h_i \right) y_2 \pmod{p}. \end{aligned} \quad (15)$$

Put $y_2 = Y_2 + Z_2$, where Z_2 is so chosen that the coefficient of Y_2 in (15) is divisible by p . Put $y_1 = Y_1 + Z_1$, where Z_1 is so chosen that the coefficient of Y_1 in (15) is divisible by p . We then have essentially

$$\sum_{i=1}^{10} a_i Q_1(x_i) \equiv rY_1^2 + sY_2^2 \equiv n \pmod{p},$$

which is solvable for every integer n since

$$r = A_2 \sum_{i=1}^5 a_i h_i^2 \quad \text{and} \quad s = A_2 \sum_{i=6}^{10} a_i h_i^2$$

are both not divisible by $p > 3$. As before we may add one more summand, $a_{11} Q_1(x_{11})$, divisible by p to insure that the primitivity condition is satisfied.

Case 2. $A_2 \equiv 0, A_3 \not\equiv 0 \pmod{p}$. Evidently this case is equivalent to the first part of the preceding case since A_2 divisible by p has the same effect in the congruence as

$$\sum_{i=1}^5 a_i h_i^2 \equiv 0 \pmod{p}.$$

Case 3. $A_2 \equiv A_3 \equiv 0 \pmod{p}$. Then

$$\sum_{i=1}^5 a_i Q_1(x_i) \equiv a_1 x_1^4 + a_2 x_2^4 + \dots + a_5 x_5^4 \equiv n \pmod{p}$$

has a primitive solution by Lemma 29 of Huston's paper.

Case 4. $A_2 \not\equiv 0, A_3 \equiv 0 \pmod{p = 4m + 1}$. Choose h_i so that

$\sum_{i=1}^5 a_i h_i^4 \equiv 0 \pmod{p}$ and $\sum_{i=1}^5 a_i h_i^2 \not\equiv 0 \pmod{p}$. This can be done since $\xi^4 \equiv 1 \pmod{p}$ has at least one root ξ such that $\xi^2 \not\equiv 1 \pmod{p}$. Hence if $(h_1, h_2, \dots, h_5)$ is a solution of

$$\sum_{i=1}^5 a_i h_i^4 \equiv \sum_{i=1}^5 a_i h_i^2 \equiv 0 \pmod{p},$$

then $(\xi h_1, h_2, \dots, h_5)$ is a solution of $\sum_{i=1}^5 a_i h_i^4 \equiv 0 \pmod{p}$ but does not satisfy

$\sum_{i=1}^5 a_i h_i^2 \equiv 0 \pmod{p}$. Use this latter set of h_i . Then we can obtain

$$\sum_{i=1}^5 a_i Q_1(x_i) + \sum_{i=6}^{10} a_i Q_1(x_i) = A_2 \left(\sum_{i=1}^5 a_i h_i^2 \right) y_1^2 + A_2 \left(\sum_{i=6}^{10} a_i h_i^2 \right) y_2^2 \equiv n \pmod{p},$$

which is solvable for every integer n since neither $r = A_2 \left(\sum_{i=1}^5 a_i h_i^2 \right)$ nor $y = A_2 \left(\sum_{i=6}^{10} a_i h_i^2 \right)$ is divisible by p .

The proof fails when A_3 is divisible by a prime of the form $4m + 3$. This gives rise to the exception in the theorem. An additional summand, $a_{11}Q(x_{11})$, can be added if necessary to satisfy the condition that our solution be primitive.

Hence for $p > 3$ we have the congruence (12) solvable for $s \geq 11$, with the one exception noted.

For $p \leq 3$ we assume that our set has the properties $S(2, 2^4)$ and $S(3, 3^2)$. This assumption reduces the discussion of this case to that of Miss Humphreys. Her proof for the quartic case, $p \leq 3$, $a_1 = a_2 = \dots = a_s = 1$ then applies to the case under discussion. Hence we have Theorem 4.

11. Proofs of Theorems 3 and 5. If $\mathfrak{S}_{0n} \geq \eta > 0$, where η is independent of n , it follows from Theorem 1 that $r(n) > 0$ when

$$n > C_{42} = ((C_{25} \alpha_0^{s/k} (a_1 \cdots a_s)^{2/k} \Gamma(s/k) / \eta \Gamma^s(1 + 1/k))^{1/B_5}.$$

The proofs of Theorems 3 and 5 are thus reduced to the proof of

LEMMA 5. *If for the cubic polynomial $s \geq 9$ and if for the quartic polynomial $s \geq 21$, then*

$$\mathfrak{S}_{0n} \geq \eta > 0,$$

where η is independent of n .

Since $M_0(p^l) \geq N_{sp}(p^l)$ we have from Lemmas 2 and 1 and Theorems 2 and 4 in the respective cases

$$\begin{aligned} (16) \quad \sum_{q|p^l} A_0(q) &= p^{-l(s-1)} M_0(p^l) \geq p^{-l(s-1)} N_{sp}(p^l) \\ &= p^{-l(s-1)} p^{(l-\gamma)(s-1)} N_{sp}(p^\gamma) \geq p^{-\gamma(s-1)} \geq p^{-l(s-1)}, \end{aligned}$$

where $t = 4$ for $P(x)$ in (3) and $t = 3$ for $P(x)$ as in (2). The final inequality holds since in the respective cases $(l \geq 4 \geq \gamma)$, $(l \geq 3 \geq \gamma)$. Then by Lemma 4 with $\epsilon = 1/8$

$$(17) \quad \sum_{q|p^l} A_0(q) = 1 + \sum_{\lambda=1}^{\infty} A_0(p^\lambda) > 1 - E_2 \sum_{\lambda=1}^{\infty} p^{-9\lambda/8} = 1 - E_2(p^{9/8} - 1)^{-1}.$$

Finally, the singular series is convergent for $s \geq (k-2)2^{k-1} + 5$ and hence by (16), (17) and Lemma 3

$$\begin{aligned} \mathfrak{S}_{0n} &= \lim_{l \rightarrow \infty} \sum_{q|p_1^{l_1} \cdots p_l^{l_l}} A_0(q) = \lim_{l \rightarrow \infty} \prod_{p \leq p_l} \sum_{q|p^l} A_0(q) \\ &\geq \prod_p \max(p^{-t(s-1)}, 1 - E_2(p^{9/8} - 1)^{-1}) \\ &\geq \eta > 0. \end{aligned}$$

UNIVERSITY OF CHICAGO.

VITA

Kenneth Smith Ghent was born in Hamilton, Ontario, Canada on June 29, 1911. He attended primary school in Battleford, Saskatchewan, and Hamilton, Ontario. He completed his high school course at Delta Collegiate Institute, Hamilton, Ontario in 1928. He then enrolled in the Honour Mathematics and Physics course at McMaster University. He there received the degree of Bachelor of Arts in May, 1932. While at McMaster he studied mathematics under Professors Findlay and Johns.

In the fall of 1932 he entered the University of Chicago and was awarded the degree of Master of Science in December, 1933.

He has studied under Professors Albert, Barnard, Bliss, Dickson, Eckart, Graves, Lane, McMillan and Sanger. To all of these he is indebted; he is particularly grateful to Professor Dickson for his inspiration and guidance in the preparation of this thesis.

